

AN E&E SPECIAL REPORT

SECURITY

Inside the Ukrainian hack that put U.S. grid on high alert

Blake Sobczak and Peter Behr, E&E News reporters

Energywire: Monday, July 18, 2016

Graphic by E&E Publishing. Photo by Oran Viriyincy, courtesy of Flickr.

Eastern Europe was blanketed in a heat wave last summer. In Kiev, Ukraine, a state of desperate resignation had set in as fighting intensified between pro-Russia rebels and Ukrainian forces to the east. Separatists closed highways and attacked ports. Meanwhile, a silent incursion had started to worm its way into the email accounts of employees at media outlets, national railroads and power distributors in the western half of the country.

The digital-era Trojan horse looked like a call to arms from the nation's embattled capital. The subject line read simply, "Mobilization."

As Ukraine's civil war raged, a few mouse clicks at three local power companies set in motion the covert intrusion. It was the first successful attempt at planting a bug, then disabling an electric grid serving hundreds of thousands of people.

SPECIAL REPORT



A four-part *EnergyWire* investigation documents how an

At 3:30 p.m. on Dec. 23, 2015, lights winked out in parts of the Ivano-Frankivsk regional capital. A minute later, another part of the grid went down. Soon, a third utility — and almost one-quarter of a million households and businesses had lost electricity.

Workers at the Prykarpattiaoblenergo, Kyivoblenergo and Chernivtsioblenergo utilities watched helplessly as cursors moved across their workstation screens at the intruders' commands, shutting

unprecedented cyberattack in Ukraine exposed troubling security gaps across the U.S. power grid and a dysfunctional cyber alert system at the U.S. Department of Homeland Security. [Click here](#) to view the report.

down substations. Other hidden commands destroyed vital equipment. The attackers were invisible and precise, and they showed the world how fragile critical infrastructure is when hacking is used as a weapon of war.

Ukraine's battle to wrest control from the hackers elevated the story of frequent blackouts in a poor country to the latest in a series of cyberattacks with implications for the United States. Months in the making, it represented an escalation in attack methods that frightened U.S. authorities and executives. The hack methodically corrupted

standard programming and subverted controls. It laid bare the work of persistent planners.

Seven months after the Ukraine attack, U.S. security officials are still trying to understand whether the much larger, and more sophisticated, North American power grid is equally as vulnerable to a determined, insidious assault. A more ominous warning has been sounded to utilities and federal agencies: Step up preparations to recover from a cyberattack that may one day break through.

Hackers didn't simply crack a code and pull the off-switches at local substations — they rendered some crucial station devices inoperable. Then, they corrupted software and servers designed to turn the power back on.

The unparalleled grid strike in Eastern Europe has led to stronger, more frustrated complaints by industry and security experts about the performance of the U.S. Department of Homeland Security as a source of rapid, actionable cyberthreat intelligence for the electricity sector. It also has raised concerns that federal guidelines applicable to the high-voltage interstate grid don't guarantee the security of local utilities that distribute power to millions of homes and businesses.

A four-part investigation by *EnergyWire* found that relationships between DHS and outside experts with deep knowledge about grid security became badly frayed in the weeks after the December hack. For several months, DHS put out conflicting internal and public messages about the dangers posed by the Ukraine hack, compounded by tug of wars around the use of closely held information inside the diffuse intelligence community.

What resulted was a slow and halting response by the U.S. government in the aftermath of the Ukraine takedown.

In an age that pits state-sponsored hackers against private companies like power utilities, critics of congressional inaction and government secrecy are starting to hammer at what they view as glaring failures around threat-sharing.

Ukraine is one of a cluster of cyberattacks in the past two years that grabbed headlines. The November 2014 attack on Sony Pictures Entertainment mushroomed into a national security and free-speech entanglement with North Korea. The U.S. Office of Personnel Management (OPM) disclosed last summer that computer breaches included the theft of Social Security numbers of 21 million Americans. Hackers also stole fingerprints of government workers and compromised security clearances.

The Obama administration in September 2015 publicly acknowledged suspicions that China was the source of the OPM breach.

In the Ukraine case, top administration officials have kept quiet, refusing to give credence to experts' widely held view that Russian hackers likely planned and executed the first-known takedown of a power grid.

Reconnaissance

The email messages snuck through the Ukrainian utility servers in droves last summer, asking employees there to "enable content" to read the attached document. When they clicked, the file unloaded the BlackEnergy attack software on their office computer systems, burrowing deep into the information

the hackers' commands to open high-voltage circuit breakers at dozens of substations across western Ukraine, knocking out power. The machines had never been programmed to question why so many users would simultaneously log in from unusual internet protocol addresses. The virtual network tied to the operational workstations asked for a username and password — nothing more — to grant unfettered access.

With credentials in hand, the attackers still had to understand Ukraine's Soviet-era electricity infrastructure to do any real damage. After all, they were dealing with three different power distribution management systems at three different companies.

At 6 p.m. on Dec. 23, the situation moved from bad to worse for one operator when the hackers cut off the backup power source to a critical control center, preventing the system from rebooting. Once merely spectators, utility workers were now blind to what was happening in the far-flung power distribution networks that had once been under their control.

Impact

The blackout itself lasted less than six hours in most places. It was hardly calamitous for Ivano-Frankivsk, which is "no Manhattan," as one Ukrainian source put it. The two other, mostly rural areas affected by the outages were similarly accustomed to power disruptions.

Many Ukrainians put up with electricity rationing for the better part of a decade following independence from the Soviet Union in 1990. More recently, war in the East has made reliable energy something of a luxury there. While western districts are more secure, critical services — hospitals, key government buildings and the like — still keep backup generators as standard practice.

December normally brings brutal cold for much of Ukraine, with the capital, Kiev, averaging just 28 degrees Fahrenheit throughout the month. But highs on the Wednesday of the cyberattack stretched into the 50s across swaths of the country, meaning the outages were less likely to endanger human lives.

Still, until that day, hackers had never carried out such a surgical strike on civilian infrastructure. And even if Ukrainians pride themselves on their resilience, no one, from Ivano-Frankivsk to Manhattan, likes living without electricity for long.

Interference

Prykarpattiaoblenergo offered the first sign the blackout was more than just a routine interruption.

The day before much of the West would celebrate Christmas Eve, the Ukrainian utility warned its customers not to call in to report power outages, so its workers could get a grip on the unfolding crisis.

“ It was a demonstration of power, maybe just field testing of the tools and the tactics. ”

Vlad Styranyan
Co-founder of the Kiev-based cybersecurity firm Berezha Security

The Ivano-Frankivsk-based company's phone lines had been swamped by a barrage of calls that investigators later traced to Russia.

This "telephone denial of service" would be bad enough during a normal blackout. But Prykarpattiaoblenergo's

technical director added that "outsiders" had tampered with the utility's control systems, forcing the company to revert to manual operations across its territory.

The hackers didn't want to switch off power only to see their work undone minutes later. They were actively

sabotaging recovery efforts, leaving no trace of doubt as to their intent.

Coercive updates went out to boxes used to translate data from grid equipment, a move that effectively turned the converters into bricks. Analysts later found that the attackers must have tested the malicious code beforehand, so they knew it would cause delicate field devices to fail.

Before calling off their assault, the online attackers left behind another nasty gift: "KillDisk" malware to wipe victims' computers and render them useless. It was the digital equivalent of kicking the power companies while they were down.

Aftershocks

At least three other energy companies in Ukraine were targeted in the campaign, but were able to stop the hackers from causing physical damage. Meanwhile, the hardest-hit power companies spent months in "manual mode," unable to trust their networks enough to go back to normal operations.

The attackers weren't done yet. In January this year, more emails made the rounds at energy companies in Ukraine, but they ditched the BlackEnergy malware in favor of a different, less sophisticated Trojan horse.

This time, the emails claimed to come from Ukraine's main electricity market overseer, the National Power Company "Ukrenergo."

"When I read through the email that [hackers] prepared for the Oblenergo companies, originating from the regulator, it was perfect," said Vlad Styran, co-founder and manager of operations at the Kiev-based cybersecurity firm Berezha Security. "There was either a lot of work behind that, or they had access to an insider" who knew the writing style and types of files normally shared by the Ukrenergo, he added.

The targeted utilities were on guard following the attacks, and no follow-up physical disruptions are known to have happened in Ukraine beyond Dec. 23.

Styran, whose day job challenges him to think about ways to break into companies as a "white hat" hacker, has suggested the Dec. 23 cyberattacks were a warning shot rather than an attempt to disable Ukraine's infrastructure indefinitely.

Among the dozens of security experts contacted by *EnergyWire*, the vast majority agreed that the level of sophistication, organization and time that went into the attack points to a state-sponsored hacking group with control system expertise.

Russia remains the most likely culprit, even though two of the three utilities harmed are majority-owned by Russian businessmen, including one reported ally of Putin. The Security Service of Ukraine wasted no time in blaming the Kremlin for the attacks. Russian authorities have yet to comment on the case.

"It was a demonstration of power, maybe just field testing of the tools and the tactics," Styran said. "That's how we can treat it. If the goal was to make harm, the targets would be completely different."

From theory to practice

The attack was a call to arms in the inchoate language of cyber warfare.

To Robert Lipovsky, who was among the first cybersecurity analysts to examine the Ukraine case, the events of Dec. 23 showed "that things such as this aren't just theoretically possible," he said, "that things like this can happen."

"It shouldn't have been so easy for the attackers," said Lipovsky, a Slovakia-based senior malware researcher at cybersecurity firm ESET.

He cited the attackers' ability to hop from utility computers on the business side over to operational workstations that directly communicated with control systems. Such a threadbare "air gap" between

operational and informational networks is not unusual in other parts of the world, he noted.

"There are definitely loopholes, generally. It's not just limited to Ukraine," he said. "This shouldn't be taken lightly."

Part 2 in EnergyWire's "The Hack" series explores the Department of Homeland Security's response to the Ukraine attack.

Twitter: [@BlakeSobczak](#) | Email: bsobczak@eenews.net

Advertisement

The essential news for energy & environment professionals

© 1996-2018 Environment & Energy Publishing, LLC [Privacy Policy](#) [Site Map](#) [Contact Us](#)

AN E&E SPECIAL REPORT

SECURITY**How DHS fell silent when a hack threatened the U.S. power grid**

Blake Sobczak and Peter Behr, E&E News reporters

Energywire: Tuesday, July 19, 2016



Homeland Security Secretary Jeh Johnson. Photo courtesy of AP Images.

Second of a four-part series. [Click here](#) to read part one.

A month after hackers blacked out power in western Ukraine, a team of U.S. security experts touched down in Kiev to piece together the extraordinary assault.

Interviews, cellphone video evidence and a crash course in Soviet-era grid equipment helped the dozen or so Americans untangle the Dec. 23, 2015, cyberattack on three utilities. The investigators traveled thousands of miles with one big question in mind: Could the methods used to hack the Ukrainian power distributors, or the hidden code behind the strike, pose a threat to the U.S. electric grid?

But two days into the five-day mission, analysts working in an opaque intelligence aggregator at the U.S. Department of Homeland Security reached their own conclusion. The Ukraine case did not pose any particular risk for U.S. systems, according to a Jan. 27 DHS memo marked "For Official Use Only."

SPECIAL REPORT

A four-part *EnergyWire*

Weeks later, a separate branch of DHS flipped that conclusion on its head, delivering the first in a series of stark warnings to electric utilities and other operators of U.S. critical infrastructure.

The conflicting and drawn-out response to the hack has triggered pointed criticism about DHS's ability to deliver cyberthreat intelligence outside the walls of government. The agency is supposed to spread the word about fast-moving online threats to the networks that underlie

investigation documents how an unprecedented cyberattack in Ukraine exposed troubling security gaps across the U.S. power grid and a dysfunctional cyber alert system at the U.S. Department of Homeland Security. [Click here](#) to view the report.

everything from the bulk power grid to car factories. But in the case of the Ukraine hack, the first of its kind, it took two months for DHS to disclose lessons from the incident and three more months to provide additional guidance accounting for the attackers' techniques.

"There was a credible threat to the U.S. grid, with realistic mitigations that could have been applied, and instead [DHS] decided to sit on the information," said Robert M. Lee, founder of Dragos Security LLC and a co-author of an influential SANS Institute analysis of the Ukraine case.

"In the midst of the first attack on a power grid that was public, there was no public word from the government," he said.

The war that had been raging in Ukraine for two years was a major source of frustration for U.S.-Russia relations. The agency was struggling to field requests from the utility industry and private analysts to share what the U.S. government considered sensitive information.

Some industry officials had an inside track on earlier attack details, including executives with security clearances and members of the CEO-level Electricity Subsector Coordinating Council, the industry's principal liaison with the U.S. government on security issues. But the broader power sector would have to wait.

The hackers in Eastern Europe had preyed upon equipment and technological vulnerabilities also present in North America's energy infrastructure, even repurposing a malware strain that was unearthed in U.S. systems in 2014.

As DHS officials kept largely quiet, utilities relied on private cybersecurity firms and media reports to fill in the blanks about the methods hackers used. Experts say the early lack of widely shared, actionable data could have left some companies exposed. And that has put DHS at the center of concerns about the effectiveness of cyberthreat-sharing from the U.S. government to the private sector, which controls the vast majority of the nation's critical infrastructure.

"If the U.S. government is seeking to achieve a real partnership with the private sector, what is their value-added proposition?" said Susan Hennessey, a fellow in national security law at the Brookings Institution and managing editor of *Lawfare*.

Unimportant or 'imperative'?

DHS was still trying to pin down details of the Ukraine attack a month after it happened.

During the on-the-ground investigation in western Ukraine from Jan. 25 to 29, DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) joined representatives from the Department of Energy, the FBI and the North American Electric Reliability Corp. (NERC), which develops and enforces cybersecurity rules for the high-voltage bulk power transmission grid.

The itinerary was secret. But the fact-finding mission came as no surprise, given that the hourslong grid takedown in Ukraine was without precedent in the brief history of cyber conflict. Private security firms had already concluded in early January that evidence pointed to computer hackers, not some other form of sabotage or human error.

Still, officials at DHS headquarters saw no reason to wait for investigators to return from Ukraine before issuing a threat

“ This incident does not represent an increase in the threat of a disruptive or destructive cyberattack ”

assessment. On Jan. 27, with the investigators on the ground, DHS's Office of Intelligence and Analysis (I&A) published an analysis titled, in bold letters, "Damaging Cyber Attacks Possible but Not Likely Against the U.S. Energy Sector."

on U.S. energy infrastructure, which I&A assesses is low.

Jan. 27 report issued by DHS's Office of Intelligence and Analysis.

The report from I&A, which reports directly to DHS Secretary Jeh Johnson, said it "is unable to confirm the event was triggered by cyber means," citing "limited authoritative reporting."

I&A is tasked with analyzing top-secret intelligence, and it's charged with being a DHS conduit to state and local authorities. Its direct access to DHS's chain of command also puts it at the center of gravity as the agency considers rising threats. But the office has faced sharp criticism from Congress about its effectiveness, and it has fought turf battles with the FBI over who is tasked with distributing information about domestic threats.

The I&A **report**, which was later leaked and published by the Public Intelligence accountability and transparency research project, concluded that "this incident does not represent an increase in the threat of a disruptive or destructive cyberattack on U.S. energy infrastructure, which I&A assesses is low."

In explaining the reassuring finding in a footnote, I&A said it was based on the earliest views of the attack expressed at a Jan. 4 meeting that included DHS and industry officials.

But the I&A outlook crumbled fast. DHS's view switched 180 degrees two weeks after the U.S. team returned home. In a February alert pushed out to electricity providers, DHS officials warned of a potential threat against utilities. The seriousness of DHS alerts to industry only escalated from there.

On March 7, the department released a detailed **breakdown** and alert about the attack and cited an "urgent need" for grid operators and other critical infrastructure owners to take "enhanced cyber measures" to protect themselves.

On the same day, Andy Ozment, DHS assistant secretary for cybersecurity and communications, and Greg Touhill, the deputy assistant secretary in the same office, stated that while there was no evidence of a Ukraine-level attack underway in the United States, it was "imperative" to raise defenses against what happened there.

The DHS alert put the risk in stark terms.

"It is the assessment of ICS-CERT that critical infrastructure [industrial control system] networks, across multiple sectors, are vulnerable to similar attacks," the alert said.

DHS officials rejected repeated requests from *EnergyWire* for interviews and information about the department's response to the Ukraine attack and any lessons the agency learned.

By spring, senior DHS officials had switched gears from silence about the threat to elevating Ukraine to a top priority.

"It is incredibly important," said Suzanne Spaulding, DHS undersecretary for the National Protection and Programs Directorate (NPPD), in an April 12 podcast interview with a Washington law firm. "We are beginning a multi-city campaign across the country to make sure we get the word to critical infrastructure owners and operators about what happened there."

Spaulding said the "good news" is that the U.S. government knows how to protect against and mitigate a Ukraine-style attack on critical control systems. "But folks have to take steps. They have to take action. They have to understand this is not just something that has the potential to affect the electric grid," but something



DHS Undersecretary Suzanne Spaulding speaks during a dialogue on cyber crime in Beijing on June 14. In an April 12 interview with a podcast housed at a Washington law firm, Spaulding said the Ukraine hack was "incredibly important." In May, five months after the Ukraine blackout, DHS held meetings with companies about the hack. She did not agree to be interviewed for this story. Photo courtesy of AP Images.

that could affect any Internet-connected critical infrastructure organization, she said.

NERC, the U.S. grid overseer, has maintained that the impact to the U.S. bulk electric power system would be blunted by best practices and binding federal critical infrastructure protection standards, the latest version of which took effect this month. But the standards rarely trickle down to small electric utilities.

"The grid in North America is larger and more diverse in the design and configuration of its equipment, including industrial control systems," NERC spokesman Martin Coyne said in response to *EnergyWire's* emailed questions. "As part of the industry's best practices, these systems run on licensed software and are routinely

screened for potential threats including malware, which is not the case in Ukraine."

A BlackEnergy link

But there is at least one known and ominous similarity between the Ukraine systems and U.S. electric utilities — the presence of BlackEnergy, a powerful, elusive intrusion malware that can give attackers a hidden opening to victims' systems. DHS has issued a series of warnings that BlackEnergy 2 has broken into the U.S. grid.

The similarities between the U.S. and Ukraine strains were so striking that DHS reposted the technical indicators in its original 2014 alert on BlackEnergy 2 to help companies root out its newer cousin, BlackEnergy 3, which was spotted on the Ukraine system.

NERC said BlackEnergy 3 has not made its way across the Atlantic.

"There is no credible evidence that the incident could affect North American grid operations and no plans to modify existing regulations or guidance based on this incident," NERC spokeswoman Kimberly Mielcarek said Jan. 7, three days after her colleagues huddled in a closed-door meeting with DHS to talk about what happened in Ukraine.

The regulator posted a confidential alert about the cyberattack, including recommendations, to members of its information-sharing portal in early February and asked U.S. utilities whether they had defenses in place against the series of weapons unleashed against Ukraine.

“ It is the assessment of ICS-CERT that critical infrastructure [industrial control system] networks, across multiple sectors, are vulnerable to similar attacks. ”

March 7 alert from DHS to electric utilities and industries.

A month later, NERC shared a public analysis of the attack prepared by experts at the SANS Institute, a Bethesda, Md.-based influential cybersecurity training and research nonprofit.

That paper concluded that "nothing about the attack in Ukraine was inherently specific to Ukrainian infrastructure." It could happen elsewhere.

Duane Highley, CEO of the Arkansas Electric Cooperative Corp., who serves as co-chairman of the CEO-level Electricity Subsector Coordinating Council, testified before Congress last week that the Ukraine event offered a case study for how government could improve information sharing with his industry.

"While the content of the classified and unclassified information from the government was very helpful, the timeliness of getting specific, actionable information to industry must be improved so that we can respond as quickly as possible," Highley said in prepared remarks before the Senate Energy and Natural Resources Subcommittee on Energy.

He elaborated on his concerns in a follow-up interview last week, describing how private-sector experts pointed out that there was a vulnerability but were initially barred from sharing the details.

"We've got to become a closer partner with the Department of Energy and DHS, and we need to continue to develop greater trust, because we are on the front lines of the war," Highley said. "It used to just be the army fighting the war; now we've got the private sector fighting the war" in cyberspace.

Highley was optimistic that information sharing would improve post-Ukraine, based on follow-up conversations with administration officials and steps to implement information-sharing legislation.

"They just need to move a little faster," he said.

In fits and starts, DHS and Congress have worked toward reorganizing the agency to prioritize its industrial cybersecurity mission, in part by renaming the nondescript National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection Agency.

SANS Institute's Lee, a critic of DHS, said the agency threatened to take legal steps to block private analysts from sharing their early findings about Ukraine on security grounds. But he drew a distinction between the agency's experts and DHS's political arms.

"They're patriots. They're doing amazing work," he said. "The problem is with the bureaucracy of the larger government, where senior government leaders do not understand the technology, they don't understand the impact, and they don't understand the threat, but they're trying to limit what is said to the community."

'Are we prepared?'

The early warnings about the Ukraine attack's threat came from private industry cyber forensic specialists. For cybersecurity researcher Chris Sistrunk, the alarm arrived on Christmas Eve in a Twitter message from a trusted colleague in his close-knit circle of security professionals, Marina Krotofil. She enclosed a link to a Ukrainian-language news article.

Sistrunk couldn't believe what she was sharing: Hackers had reportedly knocked out power to hundreds of thousands of Ukrainian electricity customers.

"We were questioning if it was a real attack or not," Sistrunk said.

When he and Krotofil found mentions of the cyberattack on power companies' public websites and Facebook pages, their suspicions inched toward certainty. The Ukraine outages

Ukraine cyberattack timeline

This *EnergyWire* timeline describes the U.S. government's response to a Dec. 23, 2015, cyberattack on the electric grid in western Ukraine. The Department of Homeland Security has come under fire from experts outside the agency for taking two months to publicly acknowledge the high risks to U.S. energy infrastructure and the agency's conflicting assessments in the weeks

looked like they really were the work of hackers.

Sistrunk dialed ICS-CERT, the government's first line of defense against cyberthreats to electric infrastructure. He also notified NERC, which runs its own secure threat information-sharing site.

He said leaving the messages was "just a good thing to do" on the chance there was a similar intrusion and takedown playing out at U.S. utilities.

Get the tactics, techniques and procedures out the door fast enough, the thinking goes, and hackers won't be able to use the same tricks twice. The sooner utilities can learn about specific vulnerabilities, the smaller the window of time during which they can be exploited.

The Cybersecurity Information Sharing Act, which Congress passed late last year, called on DHS to strengthen distribution of classified cyberthreats and bring information sharing up to "machine speed." This spring, the department launched its Automated Indicator Sharing (AIS) capability to cut out the need for phone calls like Sistrunk's in the future. Only a few electric utilities are participating in the new venture at this point. The power industry's main source of cyberthreat information from the government is the Energy Department.

Such machine-to-machine warning tools work best when fed with concrete data: Which URLs have been hijacked? What internet protocol addresses are the hackers known to be using?

A few of these clues emerged as the dust settled and the lights came back on in western Ukraine. On Jan. 11, DHS published digital signatures that could be used to search for the malicious BlackEnergy payload thought to have been used during the course of the attack.

"We cannot confirm a causal link between the power outage with the presence of the malware," the agency said, adding that it still "strongly encourages" companies to look for BlackEnergy.

But there was much more to the Ukraine attack than strings and conditions, zeroes and ones. This was not a threat that could be spooled through a computer, diagnosed instantly or

following the attack.

DEC. 23, 2015

Hackers trigger power outages across western Ukraine, the first act of cyber warfare to take down a power grid.

JAN. 4, 2016

Officials at the U.S. Department of Homeland Security and U.S. grid operators, through the E-ISAC group, meet to discuss the attack.

JAN. 7, 2016

The North American Electric Reliability Corp. (NERC) tells *EnergyWire* "there is no credible evidence that the incident could affect North American grid operations." Issues no guidance.

JAN. 9, 2016

The SANS Institute, a top group of independent cyber analysts, concludes the Ukraine outages were a well-planned attack on the grid.

JAN. 11, 2016

DHS's high-level cyber response team, ICS-CERT, reissues a 2014 warning about BlackEnergy malware. The group says it "cannot confirm" BlackEnergy played a role in Ukraine, but it "strongly encourages" U.S. companies with potential exposure to search for the cyber bug.

JAN. 25, 2016

A team of U.S. cybersecurity experts starts a four-day visit to Ukraine to investigate the grid attack. DHS, the Energy Department, the FBI and NERC are all represented.

JAN. 27, 2016

With investigators still on the ground, DHS's Office of Intelligence and Analysis finds the Ukraine attack "does not represent an increase in the threat" of an attack on U.S. energy infrastructure.

quickly tamed. The threat was distinctly human, down to the bogus telephone calls designed to hamper the Ukrainian power utilities' ability to respond.

Brookings' Hennessey said DHS's assessment likely evolved as the focus shifted from the immediate attack to its broader implications, though she, too, took issue with the delay.

"It's the natural way that the U.S. government tends to respond to threats: first, in a very specific sense, because that's where the most rapid response potentially is needed," said Hennessey, who formerly worked in the Office of General Counsel at NSA. "Then they move on to the larger questions: What about the electric grid in general? What about critical infrastructure in general? Are we prepared?"

"I think DHS was shaken by the outcome of that inquiry," she said.

5.8 out of 10

The limitations of DHS's capacity to navigate cyberthreats may have stemmed from diplomatic sensitivities and bureaucratic hurdles.

DHS was only able to visit Ukraine with a green light from Kiev, according to sources with knowledge of the inquiry.

"Given that this was politically sensitive, and who the likely perpetrator was, and that the U.S. was asked to come in, all of that tempered what could be said to the public," said one informed industry official.

Sources also said DHS analysts were hampered by the Ukraine government's reluctance to publicly broadcast details of the attack. Ukraine's worries are evident from its utilities' about-face on the news blasts that went out in the immediate aftermath of the hack. Kyivoblenergo, one of the three electricity distribution companies that hackers hit hardest, circulated an announcement warning that "third parties" had made "illegal entry" into its control systems. The utility later deleted the Dec. 24 post.

Since then, Ukrainian authorities have been quick to pin the cyberattack on Russia while avoiding detailed discussions of its causes and

FEB. 2, 2016

NERC alerts members of E-ISAC to the Ukraine threat. It asks utilities whether they have taken measures to block a similar attack.

FEB. 12, 2016

DHS goes into detail about the specifics on the Ukraine attack, but the analysis is only shared on a private, secure alert portal.

FEB. 25, 2016

Two months after the attack, DHS posts its first public alert addressing the Ukraine hack and "strongly encourages" U.S. utilities to assess their safeguards against the attack methods.

MARCH 2, 2016

ICS-CERT issues a fifth and final update to its 2014 warning about BlackEnergy.

MARCH 7, 2016

DHS upgrades the for-official-use-only Feb. 12 warning with a long analysis of the attack. The agency declares an "urgent need" for U.S. utilities to protect themselves.

MARCH 18, 2016

SANS and E-ISAC find that "nothing about the attack in Ukraine was inherently specific to Ukrainian infrastructure."

APRIL 12, 2016

DHS Undersecretary Suzanne Spaulding calls the Ukraine case "incredibly important" during a weekslong, multi-city tour to get the word out to operators of utilities and other infrastructure.

APRIL 21, 2016

Senior Russian and U.S. government officials kick off a two-day meeting in Geneva "to discuss issues of

implications. One cybersecurity expert involved in the investigation declined comment, saying, "We try not to raise this topic anymore." The attack is dead and gone, the thinking goes – any takeaways have long since been debated, adopted or cast aside.

But many of the technical lessons took more time to trickle down to U.S. utilities.

On May 31, more than five months after the Ukraine blackout, DHS posted a **warning** about a commonly used piece of hardware.

In its advisory, DHS described a security glitch in a 7400-series Moxa device designed to translate serial communications in industrial environments to the modern Ethernet protocol. Moxa devices are widely deployed across the United States and worldwide, including in electric substations.

The vulnerability in question was hardly a slam-dunk, according to DHS, which ranked its severity a 5.8 on a 10-point scale. "Crafting a working exploit for this vulnerability would be difficult," the agency's Industrial Control Systems Cyber Emergency Response Team concluded, without mentioning Ukraine.

Yet on Dec. 23, remote hackers managed to disable dozens of the devices in the first-of-its-kind cyberattack on Ukraine's power grid.

Once corrupted by malicious firmware updates, the devices were impossible to repair. Grid operators in Ukraine had to buy and install brand new serial-to-Ethernet converters across affected substations.

Moxa has since stopped producing the UC 7408-LX-Plus device with the critical flaw.

To SANS's industrial cybersecurity expert Lee, DHS's response to the Moxa problem defied explanation.

"We know for a fact that the adversary took advantage of a vulnerability to overwrite the firmware on a Moxa device during a nation-state cyberattack on the power grid," he said. "And how does DHS classify it? 'It would take a really skilled attacker to do this, and we're giving it a 5 out of 10 for vulnerability rating.' What?"

Moscow, maybe

DHS's website is littered with warnings about insecure industrial products coming from big manufacturers like Siemens and Schneider Electric down to smaller companies like Malaysia-based Ecava.

In written testimony before the Senate Armed Services Committee earlier this year, U.S. Director of National Intelligence James Clapper listed threats from "cyber and technology" on Page 1.

"Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems," he said.

Clapper didn't hesitate to name names. "Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny," he said later in the annual report.

Despite the hint, no senior U.S. official has laid the blame for the Ukraine cyberattacks on Russia.

concern" about cybersecurity.

MAY 31, 2016

DHS issues more warnings about vulnerabilities to U.S. infrastructure based on the Ukraine attack.

JUNE 17, 2016

U.S. Vice President Joe Biden announces plans to commit \$220 million in new assistance to Ukraine, including improved cybersecurity for energy systems.

View the report page for [a glossary of terms](#). Timeline by E&E Publishing.

The Dec. 23 attack "serves as a wake-up call for all types of countries, especially countries like the U.S., where everything is connected," said Nadiya Kostyuk, a fellow at the EastWest Institute's Global Cooperation in Cyberspace Initiative. "And I do hope that the countries discussing potential ways of cooperating move a little faster on these types of issues."

In its Jan. 27 report, DHS's intelligence office came closest to pinning the attack on Russia, but experts don't want hand-wringing over attributing cyberattacks to come at the expense of communicating the tactics behind them.

"Government needs to understand that asset owners need to know quickly the technology behind [an attack], not whodunit," said Marcus Sachs, senior vice president and chief security officer of NERC, at a grid security event last week in Washington, D.C., noting that the two priorities are sometimes "tugging at each other."

He said that events "like Ukraine help us get closer to that kind of understanding; I think we still have a long way to go."

The third story in EnergyWire's Hack series examines how U.S. cybersecurity rules might have fared against a similar attack against the U.S. grid.

Twitter: [@BlakeSobczak](#) | Email: bsobczak@eenews.net

Advertisement

The essential news for energy & environment professionals

© 1996-2018 Environment & Energy Publishing, LLC [Privacy Policy](#) [Site Map](#) [Contact Us](#)

AN E&E SPECIAL REPORT

SECURITY

Grid hack exposes troubling security gaps for local utilities

Peter Behr and Blake Sobczak, E&E News reporters

Energywire: Wednesday, July 20, 2016



Graphic by E&E Publishing. Photo by D. Sinclair Terrasidius, courtesy of Flickr.

Third of a four-part series. [Click here](#) to read part one and [here](#) for part two.

When Washington state utility executive Benjamin Beberness dug into what was behind the crippling cybersecurity blackout in Ukraine, the details were chilling, not only because of their malevolent nature but because of how familiar those details were to Beberness.

In early spring of 2015, a "red team" of National Guard cyber experts had taken just 22 minutes to break into Beberness' electricity company, the Snohomish County Public Utility District, north of Seattle. Beberness had invited them in to test the utility's defenses.

"The cyberattack chain that the National Guard used against us, it's almost verbatim what happened in Ukraine," said Beberness, the utility's chief information technology officer.

SPECIAL REPORT



A four-part

EnergyWire investigation

At the Everett, Wash., utility and at the Ukraine *oblenerg* power companies, employees recklessly clicked on a phishing email with concealed malware that took the attackers inside the utility's business computers. "It only took one click for somebody to get in," Beberness said of his utility's fate. Once in, the Guard cyber experts found pathways into a test operations network that mirrored the Snohomish control system. After Seattle's power system, Snohomish is the second largest publicly owned utility in the state, with nearly 340,000

documents how an unprecedented cyberattack in Ukraine exposed troubling security gaps across the U.S. power grid and a dysfunctional cyber alert system at the U.S. Department of Homeland Security. [Click here](#) to view the report.

customers.

The National Guard exercise prompted new cyberdefense strategies at Snohomish. But the utility's experience gets at the heart of a lingering issue inside the energy and security communities: What if the Ukraine attack had actually hit the United States?

The answer depends on what part of the U.S. power system we're talking about, according to industry officials and cyber experts interviewed by *EnergyWire* for this [series](#). It also depends on who's regulating the corners of the grid, stretching from coal-fired power

stations in Kentucky and Great Plains wind farms to the power lines lighting up the greatest cities and the smallest whistle-stop rural towns.

The 450,000-mile network of U.S. electric generating plants and high-voltage transmission lines crossing the country is subject to mandatory federal critical infrastructure protection (CIP) rules written by the industry-led group charged with creating standards for grid operators, the North American Electric Reliability Corp. (NERC), and approved by the Federal Energy Regulatory Commission. The detailed rules are backed by audits and potential \$1-million-a-day fines for serious breaches.

Closer to homes and businesses, the 3,300 distribution utilities that deliver power to customers over and under U.S. streets are predominantly governed by voluntary cybersecurity best-practice policies established by state utility commissions, city councils or cooperative utility boards.

Federal cyber regulations would have been far more protective of the high-voltage interstate system than the porous defenses in Ukraine had been there, some leading U.S. experts say. "Our security controls in North America are very different" from Ukraine's, said NERC CEO Gerry Cauley at a congressional hearing in April. "In the unlikely event of a successful cyber or physical attack, I believe that we are well prepared."

In February, NERC sent a confidential survey to power companies on whether they were defending against the tactics used in Ukraine. And earlier this month, the grid overseer started conducting NERC-supervised compliance audits to get more information on the state of the grid.

Achilles' heel

But the federal rules don't specifically apply to the local U.S. distribution utilities, the part of the grid we all pull power from when the lights come on in the morning. This was the same corner of the electric grid hackers hit in Ukraine.

Michael Assante of the SANS Institute, a Bethesda, Md.-based cybersecurity training group, who co-authored a definitive report on the Ukraine attack, notes U.S. local and regional distribution utilities don't follow the federal critical infrastructure cyber rules, the CIP standards. Smaller utilities are exempt because of their size.

"There would be very few differences [between U.S. and Ukraine vulnerabilities] at the distribution level," said Assante, NERC's former security chief.

"A lot of people recognize this is almost the Achilles' heel of the electrical sector," said Mark Weatherford, chief cybersecurity strategist at vArmour, a data security firm, and former deputy undersecretary for cybersecurity at the Department of Homeland Security. "From a government and policy perspective, CIP standards do not apply to distribution."

Duane Highley, an executive at an electric co-op in Arkansas and co-chairman of the industry's national cybersecurity coordinating committee, said, "It's my belief that we'll find a large number of smaller utilities certainly that are not CIP compliant because they are not required to be." That's his personal opinion, he added. "That means that some of these power companies have the kinds of vulnerabilities that attackers preyed on in the Ukraine. Those are deficiencies that will need to be corrected to ensure we don't have

“ A lot of people recognize this is almost the Achilles' heel of the electrical sector. From a government and policy perspective, CIP standards do not apply to distribution. ”

Mark Weatherford
Chief cybersecurity strategist at vArmour

those kinds of attacks.”

Highley says a successful Ukraine-style attack on a small U.S. distribution utility by itself would not threaten the interstate transmission network. But it could paralyze that utility's city.

Ukraine should be a constant concern for state commissioners,

said one regulator in the densely populated Northeast. “If nothing else, it is a wake-up call to jurisdictions, states and to all of us,” said Richard Mroz, president of the New Jersey Board of Public Utilities, who chairs the cybersecurity policy panel for the National Association of Regulatory Utility Commissioners, the regulators of the nation's power distribution utilities.

New Jersey has among the most advanced state-level cybersecurity policies in the country, requiring state-regulated utilities to create programs to find and deal with cyber risks to critical systems, conduct risk assessments, carry out attack response and recovery exercises, and report cyber incidents.

“We feel very fairly confident that with what we have put in place here in New Jersey, what our companies are doing, there is a good chance our companies would have detected that threat,” Mroz said. But he added, “I can't tell you with complete confidence it would have.”

John Dickson, principal at the network security firm Denim Group Ltd., who has consulted for electric co-ops and investor-owned utilities in the past, said an attack on U.S. grid companies is likely to come from nation-backed cyber forces. “They're going to be a sophisticated and sustained threat, with lots of resources. When that's the scenario, which electric co-ops are really ready to withstand that level of a threat?”

Despite alarms from the cyberattack in Ukraine in December, “some smaller guys, co-ops, haven't changed behaviors.” Unlike banking or big retailers, many electrical utilities “do not have the daily threat that merits management team focus,” Dickson said.

Ukraine showed that “this is not theoretical anymore -- this is real,” Dickson said.

Would CIP rules have worked?

The security of the grid's top level, the network of power plants and high-voltage transmission lines, is governed by the voluminous federal critical infrastructure security rules, known as the CIP standards, now in their sixth version. Some outside experts say those standards would likely block or reveal a Ukraine-style attack in the United States, provided power companies met the letter and spirit of the rules.

“It's hard to make the case that CIP isn't making a difference,” said SANS Institute manager Ted Gutierrez.

“A compliant NERC CIP program would almost certainly have kept this attack from succeeding,” said Terry Schurter, vice president for NERC solutions at the consulting firm SigmaFlow in Plano, Texas. But, he added, “it depends a lot on execution.”

“I don't pretend that NERC CIP is perfect, far from it,” Gutierrez wrote in a blog post. The strength of the CIP “will always depend on specific design considerations and will be subject to human error, system malfunction, and attacker ingenuity.”

One CIP requirement that could have made a big difference is CIP-005, Gutierrez and Schurter said. It requires systems covered by the rules to be sheltered within a regulated utility's “electronic security

perimeter," with minimally controlled entry points, Schurter said.

Operators needing to have remote access to controls inside the perimeter must have two totally different authenticating proofs of identity, such as a PIN plus a smart card or an iris scan device, for example.

**“ This is not theoretical
anymore -- this is real. ”**

John Dickson
Denim Group Ltd.

The CIP rule requires at least two proofs that "you are who you say you are and you have rights to be where you want be," Schurter said. "That wouldn't necessarily guarantee you would obviate the attack. But the whole concept around NERC CIP is to cover all the points, because the accumulation is so hard to get past even if you are really frickin' good."

The Ukraine utilities, in contrast, allowed operators to access grid controls remotely from outside computers, requiring only a single password. The attackers found and hijacked some of the operators' sign-on credentials and were on their way.

Hunting BlackEnergy

But the CIP requirements would not have blocked the opening move of the Ukraine attack: the phishing wave of bogus emails aimed at corporate information technology networks on the business side of the Ukraine utilities. CIP rules don't apply to utility business systems.

"There is nothing CIP does that prevents people from coming into the corporate network and completely infecting it," said Tom Alrich, manager for enterprise risk services for Deloitte Advisory in Evanston, Ill. "Once the corporate network is fully infected, then they're going to find a way to get into the substations one way or another."

While the CIP standards are particular in some places, elsewhere they give utilities leeway. For example, CIP rules do not specifically require regulated utilities to remove the BlackEnergy malware that the Ukraine attackers primarily used to build secret "backdoors" from their business computers into the Ukraine utilities' control systems, in order to seize control of the operators' workstations, experts said.

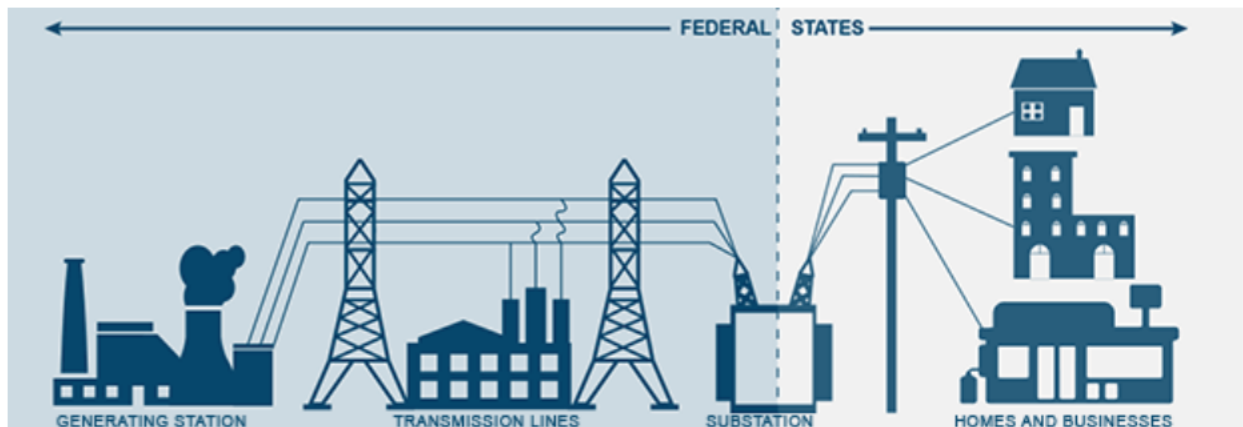
The Department of Homeland Security alerted U.S. utilities in February that BlackEnergy was suspected as an infection agent in the Ukraine incident. This followed other DHS alerts that BlackEnergy versions have been present in many places in U.S. critical infrastructure for several years at least.

In the DHS February alert, the department said it "strongly encourages" utilities to look for that malware. But DHS has no authority to order the search, and CIP rules don't require federally regulated utilities to heed that advice, although industry officials say they are confident most did.

"As far as the BlackEnergy piece goes, BlackEnergy3 in particular, it's not the easiest thing to find. Your anti-viruses aren't going to pick it up," said Jake Williams, founder and principal consultant at Rendition InfoSec LLC, who has analyzed some of the Ukraine attackers' malware.

"The folks that put this together had pretty good anti-virus evasions built in. Basically, this requires you to be performing network monitoring," Williams said of the Ukraine attack.

The electric grid



[+] The 450,000-mile network of U.S. electric generating plants and high-voltage transmission lines crossing the country is subject to mandatory federal critical infrastructure protection rules written by the industry-led group charged with creating standards for grid operators, the North American Electric Reliability Corp., and approved by the Federal Energy Regulatory Commission. The detailed rules are backed by audits and fines for serious breaches. Closer to homes and businesses, the federal rules don't apply to local U.S. distribution utilities, the same corner of the electric grid that hackers hit in Ukraine. The 3,300 distribution utilities in the United States that people pull power from when they turn on the lights are predominantly governed by voluntary cybersecurity best-practice policies established by state regulators, city councils or cooperative utility boards. Graphic by E&E Publishing.

"You have to have some mechanism to begin identifying what passed your defenses in the first place, the continuous monitoring piece: Which devices are talking to which other devices, how much data is being transferred?" he said. "That was missing in the Ukrainian power distribution network."

A capable monitoring program could have spotted all the abnormal computer traffic secretly traveling back and forth between the attackers and the Ukraine systems they had infected, months before the final attack, Williams said. "Few U.S. utilities do it now. It's the exception we see and not the rule."

Assante of the SANS Institute agreed. "You need to look at anything trying to communicate out. We find that isn't very commonplace" in the United States. "There is a requirement to conduct secure monitoring. It's not very prescriptive about what needs to be monitored, and how. So there is a blind spot."

CIP-007 requires that regulated utilities "deploy method(s) to deter, detect, or prevent malicious code." The rules don't specify how. That puts the responsibility on each utility to show NERC-approved auditors that they are meeting these requirements, said Lew Folkerth, principal reliability consultant for ReliabilityFirst Corp., in the RF newsletter for March and April. Folkerth's organization is one of the regional grid operating firms auditing CIP compliance.

Although the CIP shield creates a basic line of defense, the overall level of security still hinges on each utility's commitment, Assante said.

"For utilities that are motivated, for those utilities that have invested in people with proper skill sets and equipped them with tools, I think they will look at this incident [in Ukraine], learn from it and do things differently," Assante said.

Utilities that aren't investing, and that don't have high management buy-in for taking cybersecurity measures or the technical skills and teams, are not likely to learn the lessons of the Ukraine attack, he added.

"If they are just doing compliance -- whatever the standard says -- and pick the paths of least resistance in satisfying a requirement, those utilities probably won't benefit from this opportunity," Assante said.

The fourth and final story in EnergyWire's Hack series explores how U.S. grid operators are weighing an old-fashioned alternative to advanced cyberdefenses, one that played a key role in Ukraine's quick recovery.

Advertisement

The essential news for energy & environment professionals

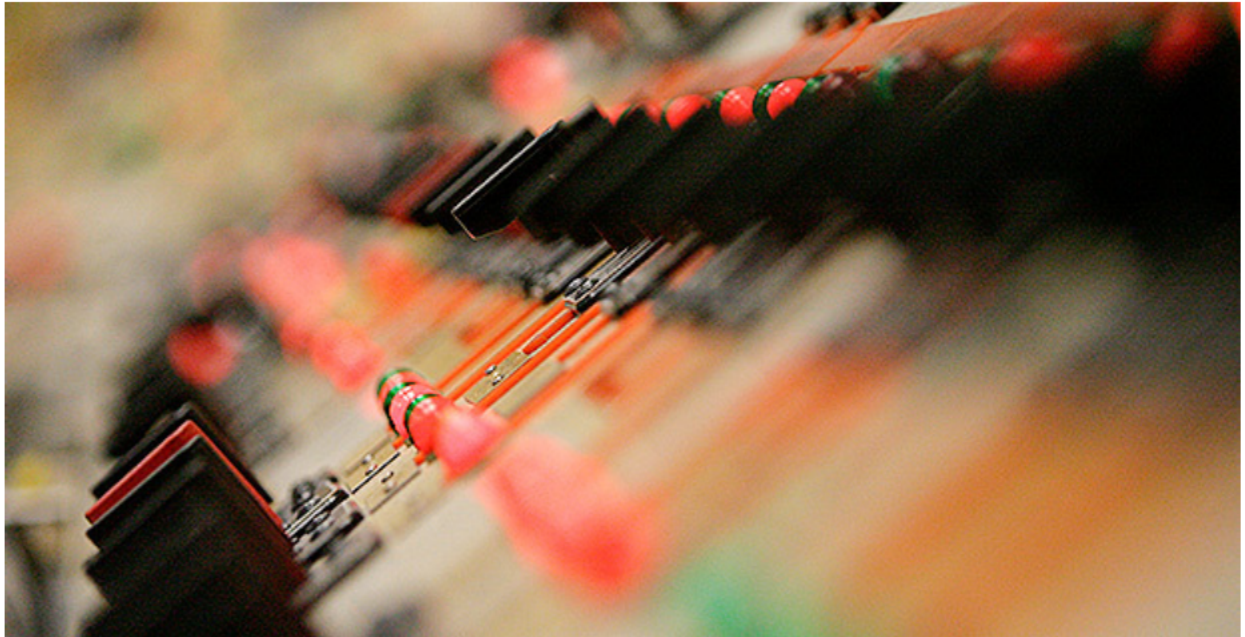
© 1996-2018 Environment & Energy Publishing, LLC [Privacy Policy](#) [Site Map](#) [Contact Us](#)

AN E&E SPECIAL REPORT

SECURITY**Utilities look back to the future for hands-on cyberdefense**

Peter Behr and Blake Sobczak, E&E News reporters

Energywire: Thursday, July 21, 2016



Experts are questioning whether cybersecurity threats against the electric grid can be overcome by analog controls. Photo courtesy of AP Images.

Fourth of a four-part series. [Click here](#) to read the entire set of stories.

The aftermath of the cyberattack in Ukraine on Dec. 23, 2015, produced two unexpected lessons that U.S. grid operators have started to take to heart.

After cutting off power to nearly 250,000 homes and businesses in western Ukraine, the cyber terrorists delivered a final punch to the gut. The hackers wrecked some of the digital controls the operators needed to restart the system remotely. An aptly named cyber weapon called "KillDisk" hidden inside the Ukraine system erased parts of the operators' startup software.

But substations across the Ukraine utilities' grid networks still had Soviet-era manual controls, so crews were able to restore power by hand within six hours.

SPECIAL REPORT

A four-part

"It was the folks who got in trucks and knew where to go and drove out and found the breakers that had been tripped through the remote access tools," said Suzanne Spaulding, undersecretary of the Department of Homeland Security's National Protection and Programs Directorate, in a blog interview.

Now, some leading U.S. grid officials, members of Congress and security experts are warning that old-fashioned protection might be

EnergyWire investigation documents how an unprecedented cyberattack in Ukraine exposed troubling security gaps across the U.S. power grid and a dysfunctional cyber alert system at the U.S. Department of Homeland Security. [Click here](#) to view the report.

needed for the more advanced U.S. power grid. Fail-safe cyberdefenses cannot be assumed in the age of the smart grid.

"We had this rush to automation over the last 15 years or so, on some level almost blind to security risks we are creating," said Scott Aaronson, executive director for security and business continuity at the Edison Electric Institute, which represents large, investor-owned utilities.

"It is good we have automation, which gives us better situational awareness. But it also increases the attack surfaces," he added, referring to the proliferation of sensors and controls that rely on

software and connect to the virus-infected internet.

"Automation is driving incredible benefits," said Michael Assante, a director of the SANS Institute, a leading cybersecurity training firm. "We've consolidated and centralized a lot. You just need to keep in mind it also lets the bad guys do the same thing."

The brutal KillDisk finale in Ukraine demonstrated how attackers could conceal destructive malware that could re-emerge unless operators effectively cleansed their control systems. The Ukraine operators failed this test, experts agree.

Joint attack

The Ukraine attackers unleashed a second weapon that has jarred U.S. cyber strategists and corporate executives: the hacker's ability to take down the utilities' electric power distribution system and also attack at least one of the utility's telephone call centers. The denial-of-service attack flooded the call center with counterfeit phone calls, preventing customers from getting through to report the loss of power, sowing more confusion and alarm among the grid operators.

"The attack in Ukraine gave us a taste of the threat to come," said Paul Stockton, managing director of Sonecon LLC and a former U.S. assistant secretary of homeland defense for the Defense Department. "That is just a small hint of the kinds of cross-sector attacks that may confront the United States."

“ We've consolidated and centralized a lot. You just need to keep in mind it also lets the bad guys do the same thing.”

Michael Assante
Director of the SANS Institute

The danger of such a one-two punch is a top-level conclusion in a new report to DHS Secretary Jeh Johnson by a cyber subcommittee of the DHS Homeland Security Advisory Council of corporate, academic and military and local government leaders.

Johnson ordered the subcommittee to address a major gap in federal cyberdefenses by finishing the DHS National Cyber Incident Response Plan (NCIRP). An interim draft of the plan was issued in 2011 but has never been completed. The lack of a final plan left key questions unsettled about how the federal government would respond to a major cyberattack on critical infrastructure, including how DHS and DOD duties would be divided, said Robert Dix Jr., a vice president for policy at Juniper Networks Inc., a Virginia-based network security firm.

The subcommittee released proposals last month calling for closer coordination of recovery plans by the

communications, electricity and financial sectors. And it called on governors to work closely with federal agencies in the wake of a large-scale cyberattack.

"What we focused on was the wake-up call that the Ukraine attack should provide to the United States, in that it reflected a simultaneous attack on the communications and energy sectors," said Stockton, a co-chairman of the DHS advisory council subcommittee.

"It is the kind of attack that will require very intense cross-sector collaboration, of the sort that the new NCIRP needs to help be able to provide," Stockton said.

The case for simplicity

The assault in Ukraine dramatizes a crucial difference between the fallout after a natural disaster damages parts of the grid and the debilitating impact of cyberattacks that leave undetected but active malware hidden inside power systems.

"That is one of the big things about the Ukraine incident," Assante noted: If other utilities are attacked, how would they know that other malware isn't still lurking after the initial attack ends?

"If they were hiding in other places, they could still be there," Assante said. "If we didn't trust our electric substations and devices anymore, how do we deal with that? How would we bring it back? Those contingencies need to be considered."

Assante and two colleagues are among the experts arguing for a return to older control methods to safeguard the most important grid operations.

"The old analog relays and circuit protection devices were as reliable as the day was long," Assante, Tim Roxey and Andy Bochman wrote last year in a paper titled "The Case for Simplicity in Energy Infrastructure," published by the Center for Strategic and International Studies.

Roxey is a vice president of the North American Electric Reliability Corp. and head of its cyberthreat-sharing program. Bochman is senior cyber and energy security strategist at the Idaho National Laboratory.

"For every major piece of grid equipment, hundreds of digital devices have evolved to support it," the authors wrote. "Remote terminal units, intelligent electronic devices, programmable logic controllers, distributed control systems, field programmable gate arrays: these are specialized computers with circuit boards, memory chips, and communications circuits, the parts sourced from innumerable suppliers, and animated via instructions coded in software. And while the hardware brings loads of complexity, it's in software that complexity truly runs wild."

One fallback position is to put more humans and nonprogrammable backup controls into systems on the most vital parts of the power grid, they said.

A generation ago, one of the authors recalled, utility systems were run by people like "Fred," he said, "who used to sleep at the substation with his dog. Give him an instruction to change a setting, and Fred would do it."

To defeat skilled cyberattackers, the most important grid components may need to rehire some "Freds" or create the equivalent with controls that are totally isolated from outside entryways, the authors argue.

Tom Fanning, chairman and CEO of Southern Co. and co-chairman of the Electric Industry Subsector Coordinating Council, the industry's CEO-level security committee, has also been looking back to the future for security.

"What are the fallback positions? The electric power industry could be run manually," Fanning said at a recent conference. "We used to do it."

Not a cure-all

A revival of older controls is not a cure-all for every situation, said Marty Edwards, director of DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

"Every entity has to evaluate that for itself," Edwards told *EnergyWire*. "It's easier to maintain some semblance of manual control when you have human resources to deploy in one small region. But if you're scattered across multiple states, that's going to be tougher. So you have to make the determination where that's important or critical."

However, the need for secure backup ways to restore power becomes vital once it's accepted that attackers may get through the best defenses, said EEI's Aaronson.

"It would be professional malpractice if we were putting all of our emphasis on 'protect, protect, protect' and not acknowledging that protection -- while incredibly important -- can't be effective 100 percent of the time," Aaronson said.

Grid operators have to think about security holistically, he said: "Not just 'protect, detect and defend', but 'respond and recover'; 'security, not just protection.'"

"Are there things we can do today to be able to operate manually in the event of an incident: Go to a degraded state simply to keep the power running?" Aaronson added, speaking at a recent cybersecurity conference. "Those are the kinds of big decisions that we are taking as a sector and in partnership with the government, to begin to do the planning for those incidents that could have an impact for a longer term on the grid," he added.

"How do we make sure the inevitable bad day doesn't become catastrophic?" he asked.

U.S. utilities -- whose cyberdefenses vary widely in sophistication and strength -- also have significantly different capabilities to recover from a major cyberattack, according to a top-level review issued in January.

A joint report by the Federal Energy Regulatory Commission and the North American Electric Reliability Corp., said a review of nine selected U.S. utilities showed that all had detailed plans for responding to and recovering from a widespread blackout. The nine utilities cooperating in the review were not named.

But the report went on to give 102 pages of ways in which the recovery plans should be bolstered, including increasing emergency startup and battery backup capacity to bring up systems after blackouts. It also called for upgrading restoration plans to account for a major change on the grid, including power plant closings. The idea is to test that recovery strategies can work in practice and confirm that spare systems and equipment will be available.

Lawmakers weigh in

The need for a fallback "manual control" has caught the attention of lawmakers in Congress.

The "Securing Energy Infrastructure Act," co-sponsored by Sen. Jim Risch (R-Idaho), chairman of the Senate Energy and Natural Resources Subcommittee on Energy, would task the Department of Energy's national laboratories with testing "analog and nondigital" control systems' ability to withstand remote cyberattacks. The legislation would free up \$11.5 million to study the issue and report back in two years.

Not everyone is convinced that the modern grid needs a hands-on makeover.

Cris Thomas, a strategist at Tenable Network Security who also goes by the hacker name "Space Rogue," called efforts to pursue a manual mode at the expense of cyberdefenses "a step backward."

"It just seems like we're spinning our wheels looking at this old stuff when we should be looking at the new," he said. Companies can apply better patches and use secure coding for state-of-the-art technologies.

Eric Spiegel, president and CEO of Siemens USA, a major developer of grid components, said at a recent cybersecurity event that much of the American grid "is old and needs to be modernized."

"A smarter grid will help prevent blackouts," he said. "But reliance on software and the Internet of Things means it gives more points of entry for people who want to harm us."

Russia's 'patriotic hacking'

The extent to which such a "smarter," more automated grid presents a risk to the United States also hinges on a candid assessment of the hackers who are capable of threatening it.

"There aren't a lot of people globally that are capable of doing what happened in Ukraine," said Thomas, noting that most in that exclusive club are U.S. allies. "In the U.S., I think that you're not going to see a similar attack against the power grid unless there are other factors involved, as well."

In Ukraine's case, the attackers were widely believed to be based in Russia, and the sophistication of the attack pointed toward state sponsorship, according to multiple experts.



Energy Secretary Ernest Moniz (left) and Sen. Jim Risch (R-Idaho) talk at the Idaho National Laboratory in August 2014. Risch is co-sponsoring legislation that would task the national labs with testing how "analog and nondigital" control systems could protect against remote cyberattacks. Photo courtesy of AP Images.

“ A smarter grid will help prevent blackouts. But reliance on software and the Internet of Things means it gives more points of entry for people who want to harm us. ”

*Eric Spiegel
President and CEO of Siemens USA*

Jason Healey, director of the Atlantic Council's Cyber Statecraft Initiative, agrees that accusing fingers point directly at Moscow. "I have almost no doubt in my mind, and that comes from a couple of lines of evidence, starting with people I trust who are savvy and not easily fooled," he said.

Some cybersecurity experts have cautiously labeled the Ukraine grid hackers a "Russian nexus," allowing for the possibility that they are advanced and organized attackers that nevertheless lack direct links to the Kremlin.

Healey suggested that such groups, if they were responsible for the power outages, still effectively work as proxies for the Russian state. "Russian 'patriotic hacking' goes back at least 10 years," he said. "If Vladimir Putin is sitting back and allowing these to happen, they don't get a pass for that."

The question then becomes whether Russia would launch an attack on U.S. utility systems, given the response that would provoke.

Representatives from the United States and Russia carried out high-level talks on cybersecurity in Geneva, Switzerland, in April, according to a senior Obama administration official. Both sides brought up the possibility of expanding information-sharing between the two countries to reduce cyber risks to networks.

It's not clear the Ukraine case was ever mentioned.

While the United States has publicly chastised and unsealed criminal indictments against hackers from rivals North Korea, Iran and even China, the administration has been quieter when it comes to Russia's role as a global hacker.

"There isn't the same level of signaling to the Russians, and I'm not sure why that is," said James Andrew Lewis, senior vice president and program director at the Center for Strategic and International Studies and a former foreign service officer who has worked on a range of cybersecurity and military issues.

Whether that silence will encourage Russia or other nations to push the boundaries of acceptable behavior in cyberspace remains to be seen. In the meantime, Lewis said, "we shouldn't rest on our laurels" when it comes to grid cyberdefense.

"Does anyone feel confident in saying that if the Russians wanted to do this to us, that they would be unable to do so?" Lewis asked. "I'm not."

Twitter: [@PeteBehrEENews](#) | Email: pbehr@eenews.net

Advertisement

The essential news for energy & environment professionals

© 1996-2018 Environment & Energy Publishing, LLC [Privacy Policy](#) [Site Map](#) [Contact Us](#)
